

On the uniform Rasmussen-Tamagawa conjecture in the CM case

Davide Lombardo *

Département de Mathématiques d'Orsay

Abstract

We prove a uniform version of a finiteness conjecture due to Rasmussen and Tamagawa in the case of CM abelian varieties. This extends the result of [2] from elliptic curves to abelian varieties of arbitrary dimension.

1 Introduction

Motivated by previous work of Anderson and Ihara [1], in [14] and [15] Rasmussen and Tamagawa have formulated (and partially proven) a series of finiteness conjectures for abelian varieties A over number fields K such that the extension $K(A[\ell^\infty])/K(\mu_{\ell^\infty})$ is both pro- ℓ and unramified away from ℓ . The strongest form of their conjecture, as stated in [15, Conj. 2], is the following uniform finiteness statement:

Conjecture 1.1. *Let*

$$\text{RT}(K, g, \ell) = \left\{ A \text{ abelian variety over } K \mid \begin{array}{l} \dim A = g \\ K(A[\ell^\infty])/K(\mu_{\ell^\infty}) \text{ is pro-}\ell \text{ and} \\ \text{unramified outside } \ell \end{array} \right\}.$$

There is a function $B(n, g)$ such that, for every number field K of degree n and every prime $\ell > B(n, g)$, the set $\text{RT}(K, g, \ell)$ is empty.

Much progress has been made on this conjecture – in particular, Rasmussen and Tamagawa themselves have proven [15] that the Generalized Riemann Hypothesis implies conjecture 1.1 for n odd – but an unconditional proof is only known for $g = 1$ and $[K : \mathbb{Q}]$ equal to either 1 or 3. More recently, Bourdon [2] has given an unconditional proof of a similar finiteness result for CM elliptic curves over arbitrary number fields:

Theorem 1.2. *(Bourdon [2]) Let K be a number field with $[K : \mathbb{Q}] = n$. There is a constant $C = C(n)$ depending only on n with the following property: if there exists a CM elliptic curve E/K with $K(E[\ell^\infty])$ a pro- ℓ extension of $K(\mu_\ell)$ for some rational prime ℓ , then $\ell \leq C$.*

The purpose of this note is to extend theorem 1.2 to CM abelian varieties of arbitrary dimension. To be more precise, by an **abelian variety of CM type** over K we mean an abelian variety A/K such that $\text{End}_{\overline{K}}(A) \otimes \mathbb{Q}$ contains an étale \mathbb{Q} -algebra of dimension equal to $2 \dim A$. We shall show the following higher-dimensional analogue of theorem 1.2:

*davide.lombardo@math.u-psud.fr

Theorem 1.3. *Let*

$$\mathrm{RT}^{\mathrm{CM}}(K, g, \ell) = \left\{ A \text{ abelian variety over } K \mid \begin{array}{l} \dim A = g \\ A \text{ of CM type} \\ K(A[\ell^\infty])/K(\mu_\ell) \text{ is pro-}\ell \end{array} \right\}.$$

There exists a function $C(n, g)$ with the following property: for every number field K of degree at most n the set $\mathrm{RT}^{\mathrm{CM}}(K, g, \ell)$ is empty for all $\ell > C(n, g)$.

As it is clear, theorem 1.3 yields a proof of conjecture 1.1 in the special case of CM abelian varieties. Notice that since CM abelian varieties acquire good reduction everywhere over a finite extension of their field of definition, and this extension can be taken of degree bounded by a constant depending only on the dimension, the condition that $K(A[\ell^\infty])/K$ be unramified outside ℓ is inessential in the CM case. In general, however, we do not expect finiteness if we both drop the ramification requirement and leave the realm of CM abelian varieties.

We conclude this brief introduction with a quick overview of the material to be covered in this article. In section 2 we show that in order to prove theorem 1.3 one only needs to deal with geometrically simple abelian varieties with multiplication by the full ring of integers of the corresponding CM field. In §3 we recall a lower bound on the degree of the division fields of CM abelian varieties (taken from [8]), while in §4 we show how a recent theorem of Tsimerman [21] gives a finiteness result for the set of CM fields that can act on g -dimensional CM abelian varieties defined over fields of degree at most n . In §5 we finish the proof of theorem 1.3, while §6 contains a few remarks on the problem of effectivity, together with a more detailed study of the case $n = 1, g = 2$.

2 Preliminary reductions

The situation is simpler if we assume that our abelian varieties have all their endomorphisms defined over K . It is thus natural to consider the following subset of $\mathrm{RT}^{\mathrm{CM}}(K, g, \ell)$:

$$\mathrm{RT}^{\mathrm{CM},1}(K, g, \ell) = \{ A \in \mathrm{RT}^{\mathrm{CM}}(K, g, \ell) \mid \mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A) \}.$$

Fortunately, as the following lemma shows, not much is lost in considering $\mathrm{RT}^{\mathrm{CM},1}(K, g, \ell)$ instead of the full set $\mathrm{RT}^{\mathrm{CM}}(K, g, \ell)$:

Lemma 2.1. *Suppose there exists a function $C^{(1)}(n, g)$ with the following property: for every number field K of degree at most n , the set $\mathrm{RT}^{\mathrm{CM},1}(K, g, \ell)$ is empty for all $\ell > C^{(1)}(n, g)$. Then theorem 1.3 holds.*

Proof. Recall that, for fixed g , there is a constant $D(g)$ with the following property: for every abelian variety A of dimension g over a number field K there exists an extension F of K , of degree at most $D(g)$, such that $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_F(A)$ (sharp bounds for $D(g)$ can be found in [18]). Set $C(n, g) = C^{(1)}(D(g) \cdot n, g)$.

Let now K be a number field of degree at most n . If A/K is an element of $\mathrm{RT}^{\mathrm{CM}}(K, g, \ell)$, then we can find a number field F such that $[F : \mathbb{Q}] = [F : K][K : \mathbb{Q}] \leq D(g)n$ and $\mathrm{End}_F(A) = \mathrm{End}_{\overline{F}}(A)$. The abelian variety A/F is then an element of $\mathrm{RT}^{\mathrm{CM},1}(F, g, \ell)$, which by assumption is empty for $\ell > C^{(1)}(D(g)n, g)$. This clearly implies that $\mathrm{RT}^{\mathrm{CM}}(K, g, \ell)$ is empty as long as $\ell > C^{(1)}(D(g)n, g) = C(n, g)$. \square

We can also restrict ourselves to geometrically simple varieties:

Lemma 2.2. *Let*

$$\mathrm{RT}^{\mathrm{CM},2}(K, g, \ell) = \{A \in \mathrm{RT}^{\mathrm{CM},1}(K, g, \ell) \mid A \text{ is absolutely simple}\}$$

and suppose there is a function $C^{(2)}(n, g)$ with the following property: for every number field K of degree at most n , the set $\mathrm{RT}^{\mathrm{CM},2}(K, g, \ell)$ is empty for all $\ell > C^{(2)}(n, g)$. Then theorem 1.3 holds.

Proof. It suffices to show that there exists a function $C^{(1)}(n, g)$ as in lemma 2.1. We claim that we can take $C^{(1)}(n, g) = \max_{g' \leq g} C^{(2)}(n, g')$. To see this, suppose by contradiction that there exists a number field K of degree at most n and a prime $\ell > \max_{g' \leq g} C^{(2)}(n, g')$ such that $\mathrm{RT}^{\mathrm{CM},1}(K, g, \ell)$ is nonempty. Let A/K be an element of this set. By definition we have $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$, so all the abelian subvarieties of A are defined over K . Let A'/K be an absolutely simple subvariety of A/K , and let g' be its dimension. It is clear that A' has complex multiplication, and that the extension $K(A'[\ell^\infty])/K(\mu_\ell)$ is pro- ℓ since it is a sub-extension of the (pro- ℓ) extension $K(A[\ell^\infty])/K(\mu_\ell)$. It follows that A' is an element of $\mathrm{RT}^{\mathrm{CM},2}(K, g', \ell)$, but this is a contradiction, because by assumption $\mathrm{RT}^{\mathrm{CM},2}(K, g', \ell)$ is empty for $\ell > C^{(2)}(K, g', \ell)$. \square

3 The case $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$

It remains to establish the existence of a function $C^{(2)}(n, g)$ as in lemma 2.2. A key step in doing so is the following proposition:

Proposition 3.1. *Let A/K be an element of $\mathrm{RT}^{\mathrm{CM},2}(K, g, \ell)$ and let $R = \mathrm{End}_{\overline{K}}(A)$. Either ℓ is at most $[K : \mathbb{Q}](g + 2)^{3(g+1)}$ or it divides the discriminant of $E := R \otimes \mathbb{Q}$.*

Proof. We shall suppose from the start that ℓ does not divide the discriminant of E , that is, that ℓ is unramified in E , and prove the claimed bound. Consider the tower of extensions $K(A[\ell^\infty])/K(A[\ell])/K(\mu_\ell)$. Since by assumption $K(A[\ell^\infty])/K(\mu_\ell)$ is pro- ℓ , this holds a fortiori for the extension $K(A[\ell])/K(\mu_\ell)$.

On the other hand, the hypothesis $\mathrm{End}_{\overline{K}}(A) = \mathrm{End}_K(A)$ entails that the action of $\mathrm{Gal}(\overline{K}/K)$ on $A[\ell]$ factors through $\mathrm{Gal}(\overline{K}/K)^{ab} \rightarrow (R \otimes \mathbb{F}_\ell)^\times$ ([17, Corollary 2 to Theorem 5]). Since ℓ is unramified in E we see that $(R \otimes \mathbb{F}_\ell)^\times \subseteq (\mathcal{O}_E \otimes \mathbb{F}_\ell)^\times$ has order prime to ℓ , hence the same is true for $G_\ell := \mathrm{Gal}(K(A[\ell])/K)$. Since on the other hand $K(\mu_\ell)/K$ is a sub-extension of $K(A[\ell])/K$, and by hypothesis $\mathrm{Gal}(K(A[\ell])/K(\mu_\ell))$ is an ℓ -group, this implies $K(A[\ell]) = K(\mu_\ell)$.

Also notice that the Mumford-Tate group of A is a subtorus of $\mathrm{Res}_{E/\mathbb{Q}}(\mathbb{G}_{m,E})$, which has good reduction at ℓ by the Galois criterion: in particular, $\mathrm{MT}(A)$ defines a torus over \mathbb{F}_ℓ , and the Galois group G_ℓ is a subgroup of $\mathrm{MT}(A)(\mathbb{F}_\ell)$. Notice furthermore that the degree $[K(\mu_\ell) : K]$ is at most $\varphi(\ell) = \ell - 1$.

We now give a lower bound for the degree $K(A[\ell])/K$. We take the notation of [8]: we denote by r the rank of $\mathrm{MT}(A)$, by μ the number of roots of unity in E , by E^* the reflex field of E , and by T_E (resp. T_{E^*}) the algebraic group $\mathrm{Res}_{E/\mathbb{Q}}(\mathbb{G}_{m,E})$ (resp. $\mathrm{Res}_{E^*/\mathbb{Q}}(\mathbb{G}_{m,E^*})$). Finally, we denote by F the group of connected components of $\ker\left(T_{E^*} \xrightarrow{N} T_E\right)$, where N is

the reflex norm. Since $G_\ell \subseteq \text{MT}(A)(\mathbb{F}_\ell)$ and ℓ is unramified in E , we see by [8, Theorems 1.2 and 1.3] that the degree of $K(A[\ell])/K$ is at least

$$\frac{1}{[\text{MT}(A)(\mathbb{F}_\ell) : G_\ell]} |\text{MT}(A)(\mathbb{F}_\ell)| \geq \frac{(1 - 1/\ell)^r \ell^r}{\mu \cdot [K : E^*] \cdot |F|^{2r}}.$$

We now give (rough) estimates for the various terms appearing in this expression:

- the degree $[K : E^*] = \frac{[K : \mathbb{Q}]}{[E^* : \mathbb{Q}]}$ does not exceed $\frac{1}{2}[K : \mathbb{Q}]$;
- the number μ of roots of unity in E satisfies $\varphi(\mu) \leq [E : \mathbb{Q}] = 2g$; since $\varphi(x) \geq \frac{\sqrt{x}}{2}$ for all positive integers x , we have $\mu \leq (4g)^2$;
- again by [8, Theorem 1.3] we have $|F| \leq 2 \left(\frac{r+1}{4} \right)^{(r+1)/2}$.

Putting everything together we find $[K(A[\ell]) : K] \geq \frac{2^{2r^2+1}}{16g^2} \cdot \frac{(\ell-1)^r}{[K : \mathbb{Q}]} (r+1)^{-r(r+1)}$.

A theorem of Ribet [16, Formula (3.5)] yields the inequality $r \geq 2 + \log_2(g)$, so that we have $2^{2r^2+1} \geq 2^9 g^2$; we thus obtain the inequality $[K(A[\ell]) : K] \geq 2^5 \frac{(\ell-1)^r}{[K : \mathbb{Q}]} (r+1)^{-r(r+1)}$, which, combined with $[K(A[\ell]) : K] = [K(\mu_\ell) : K] \leq \ell - 1$, leads to $\ell - 1 \geq 2^5 \cdot \frac{(\ell-1)^r}{[K : \mathbb{Q}]} (r+1)^{-r(r+1)}$, and finally to

$$\ell - 1 \leq \left(\frac{[K : \mathbb{Q}]}{32} \right)^{1/(r-1)} \cdot (r+1)^{r(r+1)/(r-1)} < [K : \mathbb{Q}] (r+1)^{3r} \leq [K : \mathbb{Q}] (g+2)^{3(g+1)}$$

as claimed (notice that $\ell - 1 < [K : \mathbb{Q}] (g+2)^{3(g+1)}$ implies $\ell \leq [K : \mathbb{Q}] (g+2)^{3(g+1)}$). \square

Remark 3.2. As it is clear from the proof, one can obtain much sharper inequalities for large g : for example, as long as $g \geq 2$, we have $r \geq 3$ by Ribet's inequality, and in the very last step of the previous proof we obtain $\ell - 1 \leq [K : \mathbb{Q}]^{1/2} (r+1)^{2r}$.

4 A theorem of Tsimerman

To finish the proof of theorem 1.3 we shall need a way to control the possible endomorphism algebras of CM abelian varieties of a given dimension. This is made possible by corollary 4.3 below, which is in turn a consequence of a recent result of Tsimerman (theorem 4.2).

Definition 4.1. Let $A/\overline{\mathbb{Q}}$ be an abelian variety of CM type. The field of moduli of A is the intersection of all the number fields F such that there exists an abelian variety A_F over F that satisfies $(A_F)_{\overline{\mathbb{Q}}} = A$.

Theorem 4.2. ([21, Theorem 1.1]) For every positive g there exist constants $k_g, \delta_g > 0$ such that if E is a CM field of degree $2g$ and if A is any abelian variety $\overline{\mathbb{Q}}$ of dimension g with endomorphism ring equal to the full ring of integers \mathcal{O}_E of E , then the field of moduli F of A satisfies

$$[F : \mathbb{Q}] \geq k_g |\text{disc}(E)|^{\delta_g}.$$

Corollary 4.3. *Let n, g be fixed positive integers. Consider the set $\mathcal{A}(n, g)$ all g -dimensional, geometrically simple abelian varieties A/K of CM type, where K is a number field of degree at most n . The set*

$$\mathcal{R}(n, g) = \{\text{End}_K(A) \otimes \mathbb{Q} \mid A \in \mathcal{A}(n, g)\}$$

is finite.

Proof. Consider an abelian variety $A \in \mathcal{A}(n, g)$ with field of definition K , and let E denote $\text{End}_{\overline{K}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$; as it is well-known, A is K -isogenous to an abelian variety A'/K with multiplication by the full ring of integers of E . Let F be the field of moduli of A' . Clearly we have $[K : \mathbb{Q}] \geq [F : \mathbb{Q}]$, and applying the previous theorem we find

$$n \geq [K : \mathbb{Q}] \geq [F : \mathbb{Q}] \geq k_g |\text{disc}(E)|^{\delta_g};$$

in particular, $\text{disc}(E)$ is bounded (in absolute value), hence there are only finitely many possibilities for $\text{End}_{\overline{K}}(A') \otimes \mathbb{Q} = \text{End}_{\overline{K}}(A) \otimes \mathbb{Q}$. As $\text{End}_K(A) \otimes \mathbb{Q}$ is a subfield of $\text{End}_{\overline{K}}(A) \otimes \mathbb{Q}$, this finishes the proof. \square

Remark 4.4. The case $g = 1$ (that is, the case of elliptic curves) of this corollary is well known, and is also a key ingredient for the arguments of [2]. To see why the case $g = 1$ follows from the classical theory of elliptic curves, consider all number fields K of degree at most n , and all elliptic curves E_1/K with (potential) complex multiplication. If E_1/K is such an elliptic curve, with complex multiplication by an order R in the quadratic imaginary field F , then the action of F on E_1 is defined over the compositum FK , and we can find an elliptic curve E_2/FK , isogenous to E_1 over FK , that has full complex multiplication by the ring of integers of F . Now it is well-known that the j -invariant of E_2 generates the Hilbert class field H of F , and on the other hand $j(E_2)$ is in FK by assumption, so it follows that

$$h(F) = [H : F] \leq [FK : \mathbb{Q}] \leq 2[K : \mathbb{Q}] \leq 2n$$

is bounded by n alone. The Brauer-Siegel theorem implies that there are only finitely many imaginary quadratic fields F with $h(F) \leq 2n$, and the finiteness of $\mathcal{R}(n, 1)$ follows.

5 Conclusion

We are now ready to prove theorem 1.3:

Theorem 5.1. *There exists a function $C(n, g)$ such that $\text{RT}^{\text{CM}}(K, g, \ell)$ is empty for all number fields K of degree at most n and all primes $\ell > C(n, g)$.*

Proof. According to lemma 2.2, it suffices to show the existence of a function $C^{(2)}(n, g)$ such that $\text{RT}^{\text{CM}, 2}(K, g, \ell)$ is empty for all number fields K of degree at most n and for all $\ell > C^{(2)}(n, g)$. Consider the set $\mathcal{R}(n, g)$ of corollary 4.3, and let Δ be the maximum of the discriminants $|\text{disc}(E)|$ for E varying in $\mathcal{R}(n, g)$.

We claim that we can take $C^{(2)}(n, g) = \max\{\Delta, n(g+2)^{3(g+1)}\}$. To see this, consider a number field K of degree at most n and an element A/K of $\text{RT}^{\text{CM}, 2}(K, g, \ell)$, and set $E = \text{End}_K(A) \otimes \mathbb{Q}$. By proposition 3.1, we have either $\ell \leq n(g+2)^{3(g+1)} \leq C^{(2)}(n, g)$ or $\ell \leq |\text{disc}(E)| \leq \Delta \leq C^{(2)}(n, g)$; in particular, $\text{RT}^{\text{CM}, 2}(K, g, \ell)$ is empty for $\ell > C^{(2)}(n, g)$ as claimed. \square

6 Some remarks on effectivity

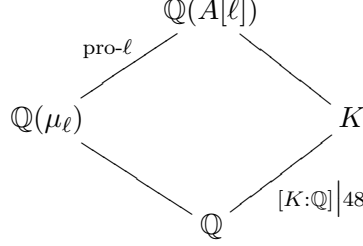
Unlike theorem 1.2, our theorem 1.3 is unfortunately non-effective: the source of this can be traced back to the proof of theorem 4.2, and more specifically to Corollary 3.2 of [21], whose proof depends on the full strength of the Brauer-Siegel theorem, which is not known to be effective at present. Notice that other parts of Tsimerman's argument also require the Brauer-Siegel theorem, but they can be made effective by using the results of [19], so [21, Corollary 3.2] is really the crux of the matter. By contrast, notice that the proof of the case $g = 1$ of corollary 4.3 sketched in remark 4.4 *can* be made effective: as it is well known, the problem of determining all imaginary quadratic fields of a given class number can be solved effectively. This fact is exploited in [2] to produce explicit bounds for the function $C(n, 1)$ for various values of n .

On the other hand, even if one is willing to assume the truth of the Generalized Riemann Hypothesis (which – as it is well known – implies effective versions of the Brauer-Siegel theorem), the argument of [21] gives for the constant δ_g of theorem 4.2 a very small value, intimately tied to a certain exponent appearing in the so-called Isogeny Theorem of Masser and Wüstholz [10] [9]; the Brauer-Siegel theorem is only used to determine the value of k_g , and has no influence on δ_g . Using the (currently) best available isogeny bound, due to Gaudron and Rémond [5], we see for example that theorem 4.2 holds for all values of δ_2 strictly smaller than 2^{-16} : clearly this number is so small that it makes it impossible in practice to use theorem 4.2 to determine the set $\mathcal{R}(n, g)$. Conditionally on GRH, sharper results are known, but none of them seems to be completely explicit at present: in the context of giving lower bounds on Galois orbits of special points on Shimura varieties, Tsimerman, Ullmo and Yafaev have proven various lower bounds on the degree of the field of moduli of a CM abelian variety (cf. for example [22] and [20]), but their results contain some non-explicit constants that seem hard to compute in practice.

Slightly different techniques – mainly coming from classical analytic number theory – can however yield results on the sets $\mathcal{R}(n, g)$ for certain small values of g and n , which in turn allows us to determine an admissible value for $C(n, g)$ – and sometimes even the optimal value – via the argument described in the previous sections. For example, we can prove

Proposition 6.1. *We can take $C(1, 2) = 163$, and this value is optimal.*

Proof. It is clear by definition that we must have $C(1, 2) \geq C(1, 1) \geq 163$, where the optimal value of $C(1, 1) = 163$ is taken from [14] (see also [2]). Consider now an abelian surface A/\mathbb{Q} admitting potential complex multiplication, and suppose first that $A_{\overline{\mathbb{Q}}}$ is isogenous to the product of two elliptic curves. Let ℓ be a prime larger than 163: we claim that $\mathbb{Q}(A[\ell])/\mathbb{Q}(\mu_\ell)$ cannot be pro- ℓ . Suppose the contrary: we shall obtain a contradiction. We shall need to rely on the results of [4], so we take the notation of that paper for the “Galois type” of our abelian variety A . Let K be a minimal field of definition for the endomorphisms of A ; by [4], we have $[K : \mathbb{Q}] \mid 48$, and K is contained in $\mathbb{Q}(A[\ell])$ by [18, Propositions 2.2 and 2.3]. In fact we know even more, namely that K/\mathbb{Q} is normal, with Galois group isomorphic to a subgroup of either $S_4 \times \mathbb{Z}/2\mathbb{Z}$ or $D_6 \times \mathbb{Z}/2\mathbb{Z}$ ([4, Table 8]). Consider now the following diagram of field extensions:



Let G_K (resp. $G_{\mathbb{Q}(\mu_\ell)}$, $G_{\mathbb{Q}}$) be the Galois group of $\mathbb{Q}(A[\ell])$ over K (resp. $\mathbb{Q}(\mu_\ell)$, \mathbb{Q}). Then $[K:\mathbb{Q}] = [G_{\mathbb{Q}}:G_K]$ is prime to ℓ , hence G_K contains a maximal ℓ -Sylow subgroup of $G_{\mathbb{Q}}$. On the other hand, $G_{\mathbb{Q}(\mu_\ell)}$ is a maximal Sylow subgroup of $G_{\mathbb{Q}}$ (notice that $\ell \nmid [\mathbb{Q}(\mu_\ell):\mathbb{Q}]$), and it is normal in $G_{\mathbb{Q}}$ because $\mathbb{Q}(\mu_\ell)$ is Galois over \mathbb{Q} . Now since all the maximal ℓ -Sylow subgroups of a group are conjugate to each other, this proves that $G_{\mathbb{Q}}$ has a unique maximal ℓ -Sylow, namely $G_{\mathbb{Q}(\mu_\ell)}$. It follows that G_K contains $G_{\mathbb{Q}(\mu_\ell)}$, hence that K is contained in $\mathbb{Q}(\mu_\ell)$. In particular, K/\mathbb{Q} is a cyclic extension, and since its Galois group is a subgroup of either $S_4 \times \mathbb{Z}/2\mathbb{Z}$ or $D_6 \times \mathbb{Z}/2\mathbb{Z}$ the group $\text{Gal}(K/\mathbb{Q})$ must be cyclic of order 1, 2, 3, 4 or 6. Depending on whether the simple factors of $A_{\overline{\mathbb{Q}}}$ are isogenous or not, the following are then the only possibilities for the Galois type of A :

1. $A_{\overline{\mathbb{Q}}}$ is isogenous to the square of an elliptic curve: then by what we have just proved, combined with [4, Table 8], the Galois type of A is one of $\mathbf{F}[C_n]$ ($n \in \{1, 2, 3, 4, 6\}$), $\mathbf{F}[C_2, C_1, \mathbb{H}]$, $\mathbf{F}[C_2, C_1, M_2(\mathbb{R})]$, $\mathbf{F}[C_4, C_2]$, $\mathbf{F}[C_6, C_3, M_2(\mathbb{R})]$, $\mathbf{F}[C_6, C_3, \mathbb{H}]$;
2. the two elliptic curves appearing as simple factors of $A_{\overline{\mathbb{Q}}}$ are non-isogenous: then the Galois type of A is one of $\mathbf{D}[C_1]$, $\mathbf{D}[C_2, \mathbb{R} \times \mathbb{C}]$, $\mathbf{D}[C_2, \mathbb{R} \times \mathbb{R}]$, $\mathbf{D}[C_4]$.

We claim that there exists a quadratic extension M of \mathbb{Q} such that A_M admits a 1-dimensional abelian subvariety defined over M (equivalently, A_M is M -isogenous to the product of two elliptic curves defined over M).

Case (2) is easy to deal with: according to [4, Theorem 4.3], only type $\mathbf{D}[C_4]$ can arise for an abelian surface A defined over \mathbb{Q} , and in this case $A_{\overline{\mathbb{Q}}}$ is simple ([4, §4.3 and 4.4]), contrary to our assumptions. We can therefore focus on case (1).

Let us first notice that, among the various subcases of (1), only cases $\mathbf{F}[C_2, C_1, M_2(\mathbb{R})]$ and $\mathbf{F}[C_6, C_3, M_2(\mathbb{R})]$ can arise for A defined over \mathbb{Q} ([4, Theorem 4.3]). As for these two Galois types, the claim about the existence of M is obvious for $\mathbf{F}[C_2, C_1, M_2(\mathbb{R})]$, because in this case K is itself a quadratic extension of \mathbb{Q} , and since all the endomorphisms of A are defined over K , so are its abelian subvarieties. For case $\mathbf{F}[C_6, C_3, M_2(\mathbb{R})]$, we know by [4, §4.5.2] that $\text{End}_K(A) \otimes \mathbb{R} \cong M_2(\mathbb{C})$, and the action of $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$ on it is determined by the fact that there is a generator g of $\mathbb{Z}/6\mathbb{Z}$ that acts on 2×2 complex matrices by the formula $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{d} & \zeta_3 \bar{c} \\ \zeta_3 \bar{b} & \bar{a} \end{pmatrix}$. It follows that g^2 acts as $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & \zeta_3^2 b \\ \zeta_3^{-2} c & d \end{pmatrix}$, so the fixed ring of g^2 is isomorphic to $\mathbb{C} \times \mathbb{C}$ (matrices with $b = c = 0$). If we denote by M the fixed field of g^2 , then M/\mathbb{Q} is a quadratic extension, and $\text{End}(A_M) \otimes \mathbb{R} \cong M_2(\mathbb{C})^{(g^2)} = \mathbb{C} \times \mathbb{C}$. Since by assumption $\text{End}_M(A)$ cannot be a number field of degree 4, it follows that $\text{End}_M(A)$ is not an integral domain, hence that A_M is nonsimple as claimed.

Let now A_1/M be an elliptic curve contained in A_M : the extension $M(A_1[\ell])/M(\mu_\ell)$, being contained in $M(A[\ell])/M(\mu_\ell)$, is pro- ℓ , but by definition of $C(2, 1)$ this is impossible for $\ell > C(2, 1) = 163$, which finishes the proof in this case.

Consider then the case of A being geometrically simple. According to [12, Theorems 2.1 and 2.2] (see also [11], [23], and [13]), if p is a prime ramified in $E := \text{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q}$, then $p \leq 61$. We claim that $\mathbb{Q}(A[\ell])/\mathbb{Q}(\mu_\ell)$ cannot be pro- ℓ for any prime $\ell > 61$. Indeed, let $\ell > 61$ be a prime, and let (E^*, Φ^*) be the reflex type of (E, Φ) , where (E, Φ) is the CM type attached to A . It is well-known that all endomorphisms of A are defined over E^* (cf. [7, Chapter 3, Theorem 1.1]), and clearly if the extension $\mathbb{Q}(A[\ell])/\mathbb{Q}(\mu_\ell)$ is pro- ℓ then the same is true for $E^*(A[\ell])/E^*(\mu_\ell)$. As in the proof of proposition 3.1, since all the endomorphisms of A are defined over E^* we know that the representation $\text{Gal}(\overline{E^*}/E^*) \rightarrow \text{Aut } A[\ell]$ factors through $(\mathcal{O}_E \otimes \mathbb{F}_\ell)^\times$, which is a group of order prime to ℓ since ℓ is unramified in E . It follows that $E^*(A[\ell]) = E^*(\mu_\ell)$, hence $[E^*(A[\ell]) : E^*] \leq \ell - 1$.

Observe now that (in the notation of the proof of proposition 3.1) we have $|F| = 1$ and $r = 3$, because this is true for all absolutely simple CM abelian surfaces; we then obtain from [8, Theorems 1.2 and 1.3] the inequality $[E^*(A[\ell]) : E^*] \geq \frac{1}{|\mu(E)|}(\ell - 1)^3$, where $\mu(E)$ is the group of roots of unity in E . Since $[E : \mathbb{Q}] = 4$, it is easy to see that $|\mu(E)| \leq 12$, whence

$$\ell - 1 \geq [E^*(\mu_\ell) : E^*] = [E^*(A[\ell]) : E^*] \geq \frac{1}{12}(\ell - 1)^3,$$

i.e. $\ell \leq 3$, a contradiction. \square

Remark 6.2. It is interesting to notice that if we only consider *absolutely simple* abelian surfaces over \mathbb{Q} , then the value 61 obtained in the course of the previous proof is optimal, as the following example shows. We know from [12] that there exists an absolutely simple abelian surface A/\mathbb{Q} , with good reduction everywhere except at 61, which admits (potential) complex multiplication by the full ring of integers of $K = \mathbb{Q}\left(\sqrt{-(61 + 6\sqrt{61})}\right)$.

The discriminant of K is 61^3 , so K is ramified at 61 only, and we have $(61)\mathcal{O}_K = \mathfrak{P}^4$ for a certain prime \mathfrak{P} of \mathcal{O}_K . The extension K/\mathbb{Q} is cyclic of degree 4, so – since it is furthermore unramified outside 61 – we see by the Kronecker-Weber theorem that it is a sub-extension of $\mathbb{Q}(\mu_{61})/\mathbb{Q}$. Writing $\text{Gal}(K/\mathbb{Q}) = \{\text{Id}, \sigma, \sigma^2, \sigma^3\}$, the CM type of A/\mathbb{Q} is $\{\text{Id}, \sigma\}$, and the reflex norm is $\Phi(x) = x \cdot \sigma^3(x)$. Recall that the reflex norm induces a group morphism $I_K \rightarrow I_K$, where I_K is the group of idèles of K , by acting on the idèles componentwise. As K/\mathbb{Q} is cyclic, K is its own reflex field, and as a consequence all the endomorphisms of A are defined over K . The class number of K is 1, so if $\omega : I_K \rightarrow \text{Gal}(K^{\text{ab}}/K)$ denotes the reciprocity map of global class field theory we see that $\omega\left(\prod_v \mathcal{O}_{K,v}^\times\right)$ is all of $\text{Gal}(K^{\text{ab}}/K)$. Hence, in order to describe the Hecke character ε attached to A_K it suffices to describe its restriction to $\prod_v \mathcal{O}_{K,v}^\times$, and by the explicit construction of [12, pp. 664 and 667] we have

$$\begin{aligned} \varepsilon : \prod_v \mathcal{O}_{K,v}^\times &\rightarrow \{\pm 1\} \\ (a_v) &\mapsto \begin{cases} 1, & \text{if } a_{\mathfrak{P}} \text{ is a square in } \mathbb{F}_{\mathfrak{P}}^\times \\ -1, & \text{otherwise} \end{cases} \end{aligned}$$

By [17, Corollary 2 to Theorem 5] we know that, since $\text{End}_K(A) = \mathcal{O}_K$, the representation $\text{Gal}(\overline{K}/K) \rightarrow \text{Aut } A[61]$ factors as

$$\text{Gal}(\overline{K}/K) \rightarrow \text{Gal}(\overline{K}/K)^{\text{ab}} \xrightarrow{\rho} (\mathcal{O}_K \otimes \mathbb{F}_{61})^\times \hookrightarrow \text{Aut } A[61],$$

and the map ρ can be described on idèle classes as

$$\rho((a_v)) = \varepsilon((a_v)) \cdot \Phi(a_{\mathfrak{P}}).$$

We claim that the image of $\text{Gal}(\overline{K}/K) \rightarrow (\mathcal{O}_K \otimes \mathbb{F}_{61})^\times$ is contained in the kernel of the natural map $(\mathcal{O}_K \otimes \mathbb{F}_{\mathfrak{p}})^\times \rightarrow \mathbb{F}_{\mathfrak{p}}^\times \rightarrow \frac{\mathbb{F}_{\mathfrak{p}}^\times}{\mathbb{F}_{\mathfrak{p}}^{\times 4}}$. Notice first that if (a_v) is any idèle class, then $\rho((a_v))$ only depends on $a_{\mathfrak{p}}$. Thus to prove our claim it suffices to check that given an element $a_{\mathfrak{p}} \in \mathcal{O}_{K,\mathfrak{p}}^\times$ the product $\varepsilon(a_{\mathfrak{p}})\Phi(a_{\mathfrak{p}})$ reduces to a fourth power in $\mathbb{F}_{\mathfrak{p}}^\times$. Notice furthermore that $\sigma \in \text{Gal}(K/\mathbb{Q})$ acts trivially on $\mathbb{Z}_{61} \subseteq \mathcal{O}_{K,\mathfrak{p}}$, so $\Phi(x) = x\sigma^3(x)$ induces the map $x \mapsto x^2$ on $\mathbb{F}_{\mathfrak{p}}^\times$. We can now prove our claim. Suppose first that $a_{\mathfrak{p}}$ is a square in $\mathbb{F}_{\mathfrak{p}}^\times$: then we have $\varepsilon(a_{\mathfrak{p}}) = 1$, and $\varepsilon(a_{\mathfrak{p}})\Phi(a_{\mathfrak{p}})$ reduces to $1 \cdot (a_{\mathfrak{p}})^2$ in $\mathbb{F}_{\mathfrak{p}}^\times$; since $a_{\mathfrak{p}}$ is a square in $\mathbb{F}_{\mathfrak{p}}^\times$, the product $\varepsilon(a_{\mathfrak{p}})\Phi(a_{\mathfrak{p}})$ is a fourth power in $\mathbb{F}_{\mathfrak{p}}^\times$ as claimed. Suppose on the other hand that $a_{\mathfrak{p}}$ is not a square in $\mathbb{F}_{\mathfrak{p}}^\times$: then $a_{\mathfrak{p}}^2$ is a square but not a fourth power, and we have $\varepsilon(a_{\mathfrak{p}}) = -1$, which again is a square but not a fourth power in $\mathbb{F}_{\mathfrak{p}}^\times \cong \mathbb{F}_{61}^\times$: the product $\varepsilon(a_{\mathfrak{p}})\Phi(a_{\mathfrak{p}})$ is then a fourth power in $\mathbb{F}_{\mathfrak{p}}^\times$ as claimed.

Let $d = 61^k a$ (with $(61, a) = 1$) be the degree of the extension $K(A[61])/K$: by what we just showed, a divides $\left| \ker \left((\mathcal{O}_K \otimes \mathbb{F}_{\mathfrak{p}})^\times \rightarrow \mathbb{F}_{\mathfrak{p}}^\times / \mathbb{F}_{\mathfrak{p}}^{\times 4} \right) \right| = \left| \mathbb{F}_{\mathfrak{p}}^{\times 4} \right| \times |\mathbb{F}_{\mathfrak{p}}|^{-3} = 15 \cdot 61^3$, so $a \mid 15$. Then since $[K(\mu_{61}) : K] \geq \frac{1}{[K:\mathbb{Q}]} \varphi(61) = 15$ and $K(\mu_{61})$ is contained in $K(A[61])$, we see that $[K(\mu_{61}) : K] = 15$ and $K(A[61])/K(\mu_{61})$ is a pro-61 extension. Finally, since K is contained in $\mathbb{Q}(\mu_{61})$, we have $K(\mu_{61}) = \mathbb{Q}(\mu_{61})$ and $K(A[61]) = \mathbb{Q}(A[61])$, and therefore $\mathbb{Q}(A[61])/\mathbb{Q}(\mu_{61})$ is a pro-61 extension. This shows, as claimed, that the constant 61 is optimal for absolutely simple abelian surfaces with CM.

As a final remark, we note that the computation of an explicit value for $C(2, 2)$ might be within reach with the current state of knowledge on quartic CM fields, and there is work in progress related to the determination of the set $\mathcal{R}(2, 2)$, see for example [3] and [6].

Acknowledgements. *I thank Abbey Bourdon for an interesting conversation that prompted me to look into this problem.*

References

- [1] G. Anderson and Y. Ihara. Pro- ℓ branched coverings of \mathbf{P}^1 and higher circular ℓ -units. *Ann. of Math. (2)*, 128(2):271–293, 1988.
- [2] A. Bourdon. A uniform version of a finiteness conjecture for CM elliptic curves. *Math. Res. Lett.*, 22(2):403–416, 2015.
- [3] F. Bouyer and M. Streng. Examples of CM curves of genus two defined over the reflex field. *LMS J. Comput. Math.*, 18(1):507–538, 2015.
- [4] F. Fité, K. S. Kedlaya, V. Rotger, and A. V. Sutherland. Sato-Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.*, 148(5):1390–1442, 2012.
- [5] É. Gaudron and G. Rémond. Polarisation et isogénies. *Duke Math. J.*, 163(11):2057–2108, 2014.
- [6] P. Kilicer and M. Streng. The CM class number one problem for curves of genus 2. *ArXiv e-prints*, November 2015.

- [7] S. Lang. *Complex multiplication*, volume 255 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1983.
- [8] D. Lombardo. Galois representations attached to abelian varieties of CM type. *ArXiv e-prints*, June 2015.
- [9] D. W. Masser and G. Wüstholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Ann. of Math. (2)*, 137(3):459–472, 1993.
- [10] D. W. Masser and G. Wüstholz. Periods and minimal abelian subvarieties. *Ann. of Math. (2)*, 137(2):407–458, 1993.
- [11] N. Murabayashi. The field of moduli of abelian surfaces with complex multiplication. *J. Reine Angew. Math.*, 470:1–26, 1996.
- [12] N. Murabayashi. Determination of simple CM abelian surfaces defined over \mathbb{Q} . *Math. Ann.*, 342(3):657–671, 2008.
- [13] N. Murabayashi and A. Umegaki. Determination of all \mathbf{Q} -rational CM-points in the moduli space of principally polarized abelian surfaces. *J. Algebra*, 235(1):267–274, 2001.
- [14] C. Rasmussen and A. Tamagawa. A finiteness conjecture on abelian varieties with constrained prime power torsion. *Math. Res. Lett.*, 15(6):1223–1231, 2008.
- [15] C. Rasmussen and A. Tamagawa. Arithmetic of abelian varieties with constrained torsion. *ArXiv e-prints*, February 2013.
- [16] K. A. Ribet. Division fields of abelian varieties with complex multiplication. *Mém. Soc. Math. France (N.S.)*, (2):75–94, 1980/81. Abelian functions and transcendental numbers (Colloq., École Polytech., Palaiseau, 1979).
- [17] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.
- [18] A. Silverberg. Fields of definition for homomorphisms of abelian varieties. *J. Pure Appl. Algebra*, 77(3):253–262, 1992.
- [19] H. M. Stark. Some effective cases of the Brauer-Siegel theorem. *Invent. Math.*, 23:135–152, 1974.
- [20] J. Tsimerman. Brauer-Siegel for arithmetic tori and lower bounds for Galois orbits of special points. *J. Amer. Math. Soc.*, 25(4):1091–1117, 2012.
- [21] J. Tsimerman. A proof of the Andre-Oort conjecture for \mathcal{A}_g . *ArXiv e-prints*, June 2015.
- [22] E. Ullmo and A. Yafaev. Nombre de classes des tores de multiplication complexe et bornes inférieures pour les orbites galoisiennes de points spéciaux. *Bull. Soc. Math. France*, 143(1):197–228, 2015.
- [23] A. Umegaki. Determination of all \mathbf{Q} -rational CM-points in moduli spaces of polarized abelian surfaces. In *Analytic number theory (Beijing/Kyoto, 1999)*, volume 6 of *Dev. Math.*, pages 349–357. Kluwer Acad. Publ., Dordrecht, 2002.